Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111
CellAntenna Corp. Request for Amendment of Section 2.807 of the Commission's Rules (47 C.F.R. § 2.807) to Allow the Use of Radio Frequency Jamming Equipment by Local and State Law Enforcement Agencies and Emergency Response Providers	)	RM-11430
Petition of The GEO Group, Inc. for Forbearance from Application of Sections 302, 303, and 333 of the Communications Act of 1934, as amended, and Sections 2.803 and 2.807 of the Commission's Rules to Allow State and Local Correctional Authorities to Prevent Use of Commercial Mobile Radio Services at Correctional Facilities	)	ET Docket No. 08-73
CTIA – The Wireless Association Petition for Declaratory Ruling Regarding the Unlawful Sale and Use of Cellular Jammers and Wireless Boosters and Repeaters	)	WT Docket No. 10-4
South Carolina Department of Corrections Request for Authorization of CMRS Jamming Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users	)	PRM09WT
Mississippi Department of Corrections Request for Authorization of Managed Access Systems Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users	)	PRM09WT

Global Tel*Link Corp. Request for Amendment of Sections 22.3(b), 1.931 and Subpart X of the Commission's Rules and Creation of New Rule(s) to Authorize a Plurality of Technical Solutions to Eradicate the Unauthorized Use of Wireless Devices in Correctional Facilities	)	PRM11WT
CellAntenna Corp. Request for Amendment of Section 20.5 of the Commission's Rules, 47 C.F.R. § 20.5, to Categorically Exclude Service to Wireless Devices Located on Local, State, or Federal Correctional Facility Premises	)	PRM11WT

COMMENTS OF TECORE NETWORKS

Carl W. Northrop
Michael Lazarus
Jessica DeSimone
Telecommunications Law Professionals PLLC
875 15th Street, NW, Suite 750
Washington, DC 20005
Telephone: (202) 789-3120
Facsimile: (202) 789-3112

Jay Salkini
Chief Executive Officer

Casey Joseph
Chief Technology Officer

Tecore Networks
7030 Hi Tech Drive
Hanover, MD 21076
Telephone: (410) 872-6238
Facsimile: (410) 872-6010

Its Attorneys

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	GN Docket No. 13-111
CellAntenna Corp. Request for Amendment of Section 2.807 of the Commission's Rules (47 C.F.R. § 2.807) to Allow the Use of Radio Frequency Jamming Equipment by Local and State Law Enforcement Agencies and Emergency Response Providers	RM-11430
Petition of The GEO Group, Inc. for Forbearance from Application of Sections 302, 303, and 333 of the Communications Act of 1934, as amended, and Sections 2.803 and 2.807 of the Commission's Rules to Allow State and Local Correctional Authorities to Prevent Use of Commercial Mobile Radio Services at Correctional Facilities	ET Docket No. 08-73
CTIA – The Wireless Association Petition for Declaratory Ruling Regarding the Unlawful Sale and Use of Cellular Jammers and Wireless Boosters and Repeaters	WT Docket No. 10-4
South Carolina Department of Corrections Request for Authorization of CMRS Jamming Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users	PRM09WT
Mississippi Department of Corrections Request for Authorization of Managed Access Systems Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users	PRM09WT

Global Tel*Link Corp. Request for Amendment of Sections 22.3(b), 1.931 and Subpart X of the Commission's Rules and Creation of New Rule(s) to Authorize a Plurality of Technical Solutions to Eradicate the Unauthorized Use of Wireless Devices in Correctional Facilities	)	PRM11WT
CellAntenna Corp. Request for Amendment of Section 20.5 of the Commission's Rules, 47 C.F.R. § 20.5, to Categorically Exclude Service to Wireless Devices Located on Local, State, or Federal Correctional Facility Premises	)	PRM11WT

COMMENTS OF TECORE NETWORKS

Tecore Networks ("Tecore"),[1] by its attorneys, submits its comments in response to the *Notice of Proposed Rulemaking* ("*NPRM*") released by the Federal Communications Commission (the "FCC" or "Commission") in the above-captioned proceedings that seeks comment on possible solutions to mitigate the skyrocketing use of contraband wireless devices in correctional facilities and related issues.[2] The following is respectfully shown:

I. INTRODUCTION AND SUMMARY

Tecore has a substantial basis in experience for informed comment in this proceeding. For over 20 years, Tecore has designed, developed and delivered scalable wireless infrastructure solutions for commercial, government, and military networks. The company has a proven track record of performance and evolution driven by an innovative software-defined approach that has

[1] These Comments are submitted on behalf of Tecore Networks and its subsidiaries.

[2] *In the Matter of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities et al.*, GN Docket No. 13-111 et al., FCC 13-58 (rel. May 1, 2013) ("*NPRM*").

evolved from the first generation of analog wireless infrastructure in the early 1990's through high-speed 4G LTE broadband being delivered today. Tecore is one of the last remaining "Made in the USA" mobile infrastructure providers, and it has succeeded in introducing its technology in a wide range of markets around the world.

The advancement of technology has enhanced and expanded mobile networks, which has given rise to an ever-increasing need to restrict access in secured areas. Realizing this need, Tecore developed the patented Intelligent Network Access Controller ("iNAC") and iCore architecture;[3] a state of the art technology and implementation methodology that lies at the heart of, and has driven, the "Managed Access Solution" concept. The iNAC addresses the serious and dangerous problem of contraband cell phones in prisons by delivering a comprehensive solution set that harnesses the very same technology that has revolutionized the wireless industry. Specifically, the iNAC forms a radio frequency umbrella around a precisely defined target area and attracts wireless devices within a certain defined range. Tecore's Managed Access Solution leverages the wireless infrastructure, components, and interfaces of the commercial network to provide system operators with the capability to selectively permit or deny communications from the wireless devices falling under the relevant umbrella. Control is provided with sufficient precision to allow for the continued support of key regulatory features, such as 911 emergency calls, regardless of device status, within the specifically defined area.

Because the iNAC and iCore solutions are uniquely positioned to address the present and future issues of wireless contraband in correctional institutions, the Tecore intelligent Managed Access Solution has received industry support in the U.S. and abroad. Tecore has been actively working with various correctional institutions to plan and deploy systems across the United

[3] The iNAC is covered by U.S. Patent Nos. US 8,254,886 and 8,437,741.

States.[4] Tecore also is ISO 9001:2008 certified, and is a three-time winner of the Global Mobile (3GSM) Award. Notably, the benefits of the Managed Access Solution developed by Tecore have been acknowledged by the FCC,[5] CTIA,[6] the top four U.S. commercial mobile operators and other carriers whose networks cover corrections facilities.[7]

---

[4] *See e.g.*, Stephanie Francis Ward, *Technology Blocks Smuggled Cellphone, But Not Approved Calls, At State Prison*, ABA JOURNAL (May 20, 2013) http://www.abajournal.com/news/article/technology_blocks_smuggled_cell_phones_but_not_911_calls_at_maryland_prison/ (describing Maryland Metropolitan Transition Center's adoption of Tecore's managed access technology, and noting that Maryland State "plan[s] to use the technology at other facilities soon."); Donny Jackson, *Mississippi Showcases Deployment To Halt Prison Cell-Phone Use*, URGENT COMMUNICATIONS (Sept. 8, 2010) http://urgentcomm.com/networks_and_systems/news/miss-deploys-cell-jammer-20100908 (after deployment of Tecore's managed access system with the Mississippi State Penitentiary, Mississippi hosted "a demonstration event highlighting the first deployed managed-access system in the U.S.," which was widely attended by public safety officials and FCC representatives).

[5] During his role as the Chief of Public Safety and Homeland Security, Jamie Barnett concluded that "this may be the answer to beating cell phones in prison." Jackson, *supra* note 4.

[6] "With support from carriers across the country, demonstrations of alternative technologies, such as managed access and cell detection, have continuously proven that they can prevent inmates from using contraband phones while ensuring public safety and consumers have service to their device." Press Release, CTIA, CTIA Statement on Press Conference in South Carolina on Cell Phones in Prison (Sept. 22, 2010) http://blog.ctia.org/2010/09/22/ctia-statement-on-press-conference-in-south-carolina-on-cell-phones-in-prisons/.

[7] *E.g.*, "AT&T continues to work closely with Tecore Networks . . . to allow commercialization of managed access solutions in prisons. Tecore's managed network access solution shows great potential for addressing the problem of contraband cell phones without jeopardizing public safety and commercial communications." Comments of AT&T submitted to NTIA, Docket No. 100504212-0212-01, 2 (filed June 11, 2010); "Managed access is the only technical choice that can properly balance the needs of prison officials, the public, public safety users of wireless telecommunications, and wireless service providers without causing harmful interference to wireless networks in the vicinity of the prison." Comments of Verizon submitted to NTIA, Docket No. 100504212-0212-01, 1 (filed June 11, 2010); "Managed access systems are a preferable solution for preventing the use of contraband cell phones within prisons because they can effectively prevent unauthorized communications without disrupting legitimate users or emergency calls and also provide additional helpful intelligence gathering capabilities." Comments of T-Mobile submitted to NTIA, Docket No. 100504212-0212-01, 8 (filed June 11, 2010); "[I]t is likely that managed access systems can be deployed in virtually all traditional commercial mobile service frequency bands for reasonable cost." Comments of Sprint Nextel submitted to NTIA, Docket No. 100504212-0212-01, 2 (filed June 11, 2010).

In sum, Tecore is at the forefront of the fight against contraband wireless devices in correctional institutions and is the industry leader in Managed Access Solutions. As a consequence, Tecore applauds the Commission for taking further steps to facilitate the development of technological solutions to combat the use of contraband wireless devices in correctional facilities nationwide. Tecore looks forward to actively participating in this important proceeding, which holds the promise of raising awareness and promoting a regulatory environment and policies that will address the growing threat to national safety and welfare. While the FCC is wise to explore multiple technological solutions to the contraband wireless device problem, as is discussed in detail below in Section IV, not all solutions are equal. Managed Access Solutions present the most comprehensive and effective approach. However, successful implementation of this optimal approach requires cooperation from all licensed carriers in the area of a correctional facility. The FCC must, therefore, create an environment that fosters cooperation, either by encouraging voluntary industry participation or by adopting appropriate rules. And, in addition to promoting and streamlining the spectrum leasing process, the Commission must also adopt guidelines on the technical and operational aspects of the Managed Access Solution to assure that managed access systems not only provide an effective deployment inside the walls of the relevant facility, but also avoid unreasonably disrupting the commercial network.

II. TIME IS OF THE ESSENCE FOR COMMISSION ACTION

Contraband device use is on the rise in our country's correctional systems. Federal, state and local agencies and institutions all have identified the use of contraband wireless devices as a major problem, and one that fosters serious crime and endangers life.[8] Inmates use contraband

[8] *NPRM* ¶¶ 4-6.

devices for a variety of illegal activities, including to organize gangs, plan escapes, facilitate drug deals, and even to initiate murders in the outside world.[9] These incidents are not isolated. They are occurring in both rural and urban areas across the United States. Unfortunately, this problem is not new, and it appears to be accelerating, not abating. The Government Accounting Office reports that the number of cell phones that were confiscated by the Federal Bureau of Prisons grew from 1,774 to 3,684 in 2010. In 2011, California correctional officers discovered more than 15,000 contraband wireless devices.[10] Tecore's operating experience in several correctional institutions confirms the alarming number of inmates who seek to initiate unauthorized communications using contraband devices.[11]

To be sure, the Commission has taken some preliminary steps to address contraband wireless device use in correctional facilities.[12] However, given the number of years that the problem has been recognized and continued to grow, much more needs to be done. The issuance of the *NPRM* is an important step in highlighting the issue and seeking solutions, but Tecore urges the Commission to recognize that time is of the essence given the serious nature of this growing national security problem. Bold, prompt action is essential. By adopting procedures that will actively encourage managed access solutions to be deployed rapidly, the Commission will be doing its part to decrease unnecessary violence and help aid the public welfare.

---

[9] *Bricking The Intruders*, THE ECONOMIST (Oct. 14, 2010) *available at* http://www.economist.com/node/17257847?story_id=17257847&fsrc=rss/.

[10] *See NPRM* ¶ 5.

[11] For instance, more than 1,300 contraband cell phones were found inside correctional facilities in Maryland last fiscal year. Ken North, *Cellphones: Preserving A Tool, Combating A Threat*, THE BALTIMORE SUN (May 23, 2013) http://www.baltimoresun.com/news/opinion/oped/bs-ed-tecore-20130523,0,1015252.story.

[12] *See NPRM* ¶¶ 7-9.

III. THE COMMISSION SHOULD ADOPT RULES TO FACILITATE THE PROMPT IMPLEMENTATION OF MANAGED ACCESS SYSTEMS

The *NPRM* takes "steps to facilitate the development of multiple technological solutions to combat the use of contraband wireless devices in correctional facilities nationwide."[13] Given the scope of the problem, and the fact that different locales have taken different approaches and have varying levels of resources to devote to the problem, a multifaceted approach is justified. However, the practical realities should not be allowed to obscure the fact that a fully implemented managed access solution – *i.e.* one that incorporates all of the licensed spectrum in the vicinity of a correctional institution – presents the most comprehensive and effective solution to the problem. The basis for this assertion is fully developed in Section IV below.

Given this reality, the Commission should adopt rules and procedures that facilitate the timely implementation of fully developed managed access solution systems. First, the Commission should adopt a definition of "managed access system" that brings the relevant deployments within the ambit of the rules. Second, and most important, the Commission must adopt policies or, if necessary, rules, that permit all of the licensed wireless spectrum in the vicinity of a correctional institution to be incorporated into a managed access system in a reasonable time, on reasonable terms and conditions. This step would inform correctional facilities that illicit wireless contraband communications are able to be prevented, regardless of the frequency range involved, and removed in a swift manner. Lastly, the Commission should streamline the regulatory approval process for spectrum leasing arrangements that are used to deploy managed access systems. Such action will enable managed access providers to deploy their systems in a swift manner, without having to jump through unnecessary procedural hoops.

[13] *Id.* at ¶ 1.

a. The Proposed Definition Of "Managed Access System" Should Be Refined

The *NPRM* contains a proposed definition of "managed access system" that seeks to capture the core functionalities of such systems. Subject to the additional refinements proposed below, Tecore generally supports the language in the proposed section 1.9003 definition of "managed access system" with one modification, as indicated by the strikethrough:

> A managed access system is a system comprised of one or more stations operating under a license, or lease arrangement entered into ~~exclusively~~ for the operation of such system, and is used in a correctional facility ~~exclusively~~ to prevent transmissions to or from unauthorized wireless devices within the boundaries of the facility.[14]

As indicated, Tecore recommends that the Commission remove the word "exclusively" both times it is used in the proposed definition because it unnecessarily restricts potential public interest benefits that may stem from such solutions. With respect to the first proposed change, the local network could potentially evolve into a local service for the prison and could be used for prison communications or the implementation of CALEA – even if the lease was originally entered into for managed access, an extension that the Commission should encourage, not restrict. "Exclusively" should also be removed the second time it is used because, in some implementations, a managed access system has capabilities other than merely preventing transmission to or from unauthorized wireless devices. Examples of these other capabilities include E911 access and CALEA-compliant interfacing, which can include communications from unauthorized devices. Also, because the managed access system identifies and allows certain authorized communications of prison officials and personnel, the proposed Commission definition is too narrow.

[14] *See id.* at Appendix A, Section 1.9003.

While the term "managed access" has been used to refer to a broad array of methods that are used to control contraband cell phones in the correctional system's vernacular, Tecore has found that there are several key elements that must be met in order for a managed access system to be comprehensive and effective. Specifically, the managed access system must: (a) cover *all* commercially deployed spectrum bands and technologies in the licensed spectrum; (b) provide an evolution path that survives the removal of 2G (GSM, CDMA 1xRTT, iDEN) from the market (both in the network and handsets); (c) provide a solution applicable for both urban and rural deployments; (d) control and manage the coverage footprint so as not to adversely impact the commercial network under normal operations; (e) support direct handling of E911 emergency calls on the managed access system with direct routing to the Public Safety Access point;[15] and (f) support direct handling of CALEA Wiretap requests with direct routing to the appropriate LEA. A managed access solution that meets these criteria will help ensure that the intended goal is met – the cessation of completed calls from contraband wireless devices from correctional facilities – without having unintended consequences.

In other contexts where public safety and welfare have been involved, the Commission has not hesitated to impose standards that are designed to ensure that technological solutions are adequate to address the problem at hand. As a consequence, there are specific rules that govern the specific manners in which E-911 services are provided, emergency alert systems are

[15] Any E911 requirement that is adopted by the Commission should not extend to the Phase 2 E911 location requirement. If the call is presented to the PSAP from the correctional institution location, it will already provide a relative proximity that allows for the location of the site of the call. Including additional location requirements would be burdensome and unnecessary.

implemented, and facility outages are reported, to name a few.[16] The Commission should take the same hands-on approach when it comes to defining the managed access systems that are being fostered by the Commission's rules. To this end, the Commission should add the above capabilities to the definition of a managed access system in order for the system to qualify under the Commission's rules.

b. The Commission Must Actively Encourage Wireless Providers To Enter Into Spectrum Leases With Managed Access System Providers

The key to the deploying a comprehensive, fully implemented managed access solution is the successful execution of spectrum subleases with each of the CMRS providers that operate on each band of spectrum in use in the vicinity of a particular correctional facility.[17] While the rule changes the Commission proposes will streamline the authorization of spectrum leasing arrangements after the fact, the proposed rules do little to encourage carriers to cooperate in the leasing of their spectrum on reasonable terms and on a timely basis.

The importance of this point cannot be overstated. If one wireless carrier's spectrum is not covered by the managed access systems, then wireless units operating on that spectrum are likely to quickly become the contraband of choice for that correctional facility. Prisons are closed systems through which news can travel fast, and the fact that a particular carrier or band of spectrum is not being managed will quickly undercut the core purpose of the managed access solution – to prevent unauthorized wireless communications from the facility.

---

[16] *See e.g.*, 47 C.F.R. § 20.18 (providing the 911 and enhanced 911 requirements for CMRS providers); 47 C.F.R. Part 11 (dictating the rules for the emergency alert system); 47 C.F.R. Part 4 (outlining outage reporting requirements).

[17] Tecore notes that a specific acceleration in the STA process does not provide a key differentiator in managed access deployments. A key measure to success of a managed access system is a defined relationship between the CMRS operator and the managed access provider. Leveraging a STA does not establish this critical relationship. *But cf. NPRM* ¶¶ 50-51.

Up to this point, managed access system providers have had to negotiate spectrum leases individually with each wireless carrier that operates over spectrum covering a particular correctional facility. Such individual negotiations include discussions regarding standard lease provisions as well as individualized terms and conditions. Even assuming that all parties are cooperative and want to conclude an arrangement, the process inevitably takes a considerable period of time. In some instances, a managed access system provider might have to negotiate with as many as seven wireless providers in certain areas.

The process is further complicated by the practical realities of the situation. Unless and until a managed access system provider knows that all spectrum in the area will be covered by the system, it is difficult to advise the correctional facility operator of the level of system performance he can expect. The prison may be hesitant to commit to the deployment without knowing what the outcome will be, and the system manager may be hesitant to commit the resources that are necessary to line up all of the leases with the carriers if the prison is not signed up. In Tecore's experience, this "chicken and egg" problem has been a major reason that more managed access systems have not been deployed. Another practical limitation is that, if each carrier is free to charge "what the market will bear" for a lease, the last holdout may be in position to extract a premium over what the other carriers have received. This not only results in uneven treatment, but also serves to discourage carriers from being the first to sign up. The net result is that deployments can be delayed, deterred or rendered uneconomic.

Solving this problem requires that a number of elements be addressed. First and foremost, carriers must either agree or, in the absence of a voluntary industry agreement, be obligated by Commission rule, to enter into leasing agreements on commercially reasonable terms and conditions. Second, a shot clock must be implemented, triggered either by (a) an

agreement between the managed access solution provider and a correctional facility manager; or (b) an agreement between the managed access solution provider and a single carrier in a market in the vicinity of a target correctional facility. The purpose of the shot clock would be to ensure that final agreements are in place between the managed access solution provider and all area carriers in a reasonable time. Third, leased access to the spectrum should be provided free of charge by the carrier to the managed access system operator in the immediate vicinity of a qualifying correctional facility because the managed access system is not able to generate CMRS commercial revenue and therefore is in a challenged revenue position. Fourth, a model lease agreement must be established so that there are standard terms and conditions addressing the core issues (*e.g.* interference protection, notifications of area residents, licensee control, etc.) in the absence of an agreement to the contrary. Each of these elements is discussed in greater detail below.

(1) Carrier Cooperation

For the past several years, Tecore has reached out to wireless carriers and carrier associations in an effort to foster a voluntary industry standard governing arrangements between carriers and managed access solution providers. Tecore is hopeful that effective voluntary standards can emerge in the course of this proceeding, particularly if the Commission actively encourages cooperation. Notably, such voluntary efforts have succeeded in the past in putting in place a series of beneficial policies and procedures that serve the public interest. For example, enlightened self-regulation has resulted in wireless carriers implementing text to 911 notifications standards,[18] programs to address the serious problems arising from stolen phones,[19]

[18] Certain wireless carriers voluntarily agreed to accelerate the availability of text-to-911, and have committed to nationwide availability by May 15, 2014. Press Release, FCC, FCC Chairman Julius Genachowski Announces Commitment By Major U.S. Wireless Carriers & (continued...)

procedures to avoid bill shock, [20] and a wireless consumer bill of rights.[21] The benefit of such voluntary measures is that they often can be implemented quickly and, because carriers have a stake in the process, compliance is not generally a problem. In most of the cases where voluntary industry standards were formulated, the Commission played a constructive role by acknowledging and encouraging the effort. Given the importance of solving the problems caused by contraband wireless devices, the Commission should be proactive here as well.

If industry efforts do not succeed in the near term, the Commission should adopt rules requiring carriers to enter into commercially reasonable subleasing arrangements upon reasonable request. Just as the Commission adopted rules requiring wireless carriers to enter into voice roaming agreements on reasonable, non-discriminatory terms[22] -- and data roaming agreements on commercially reasonable terms[23] -- the Commission has the authority to order

---

(...continued)

Public Safety Leaders To Accelerate Nationwide Text-to-911 Services; Calls For Continued Engagement With FCC On Next-Generation 9-1-1 Initiatives (Dec. 6, 2012) http://www.fcc.gov/document/chairman-genachowski-announces-commitments-accelerate-text-911.

[19] CTIA and certain wireless providers developed procedures to help deter smartphone thefts and protect consumer data, which was subsequently applauded by the FCC. Press Release, CTIA, U.S. Wireless Industry Announces Steps to Help Deter Smartphone Thefts and Protect Consumer Data (April 10, 2012) http://www.ctia.org/media/press/body.cfm/prid/2170.

[20] Certain wireless carriers have voluntarily committed to provide free alerts to consumers before and after the subscribers reach monthly limits on voice, data and text. *See* Press Release, CTIA, CTIA-The Wireless Association, Federal Communications Commission and Consumers Union Announce Free Alerts to Help Consumers Avoid Unexpected Overage Charges (Oct. 17, 2011) http://www.ctia.org/media/press/body.cfm/prid/2137.

[21] CTIA Consumer Code For Wireless Service, http://www.ctia.org/content/index.cfm/AID/10352.

[22] *Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers*, Report and Order and Further Notice of Proposed Rulemaking, WT Docket No. 05-265, 22 FCC Rcd 15817, 15818 ¶ 1 (2007).

[23] *Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers and Other Providers of Mobile Data Services*, Second Report and Order, WT Docket No. 05-265, ¶ 40 (2011).

carriers to enter into commercially reasonable subleasing agreements for the limited purpose of facilitating managed access systems.

(2) Shot Clock

Because there are multiple elements that must come together in a common time frame for a managed access solution to become fully implemented, an agreement delayed can be an agreement denied. Actions in several other contexts have proven the value of so-called "shot clocks" to foster the timely conclusion of commercial agreements of this nature. For instance, local zoning authorities have been made subject to shot clocks in connection with action upon wireless siting proposals.[24] A timetable also is in place for carriers to meet number porting requests.[25] Again, Tecore is receptive to the idea of allowing industry representatives to participate in arriving at a suitable schedule. The key is to have an outside limit so that timely implementation of managed access solutions is possible.

The logical starting time for the shot clock is the earlier of (a) the date when a managed access solution provider enters into a contract with a correctional facility; or (b) the date when the managed access solution provider enters into an initial agreement with an area carrier pertaining to spectrum covering a particular facility. Either event is sufficiently indicative of a seriousness of intent to merit starting the clock.

---

[24] The FCC has adopted a shot clock of 90 days for collocation and 150 days for new tower construction for local zoning authorities to act on tower siting requests. *See In the matter of Petition for Declaratory Ruling to Clarify Provisions of Section 332(c)(7)(B) to Ensure Timely Siting Review and to Preempt Under Section 253 State and Local Ordinances that Classify All Wireless Siting Proposals as Requiring a Variance*, Declaratory Ruling, WT Docket No. 08-165 (rel. Nov. 18, 2009)

[25] "Simple" number porting must be completed in one business day, while non-simple ports must be completed in four business days. *See In the Matters of Local Number Portability Porting Interval and Validation Requirements, Telephone Number Portability*, WC Docket No. 07-244, CC Docket No. 95-116, Report and Order (rel. May 20, 2010).

(3) Free Access

It is no surprise that the price term of a contract is often the sticking point that either delays or prevents an agreement. Therefore, specific pricing standards should be adopted and monitored by the Commission for managed access leases. Tecore proposes that these leases should be provided free of charge solely for the purpose of managed access with the understanding that the geographic area covered by the lease will be limited to the immediate environs of the correctional facility. Because managed access, under the Commission's proposal, will be provided as PMRS for the purposes of preventing calls rather than completing them, these systems will not be generating commercial revenue as a CMRS system, which creates inherent revenue limitations.[26] And, while the managed access service provider might be able to charge the correctional facility, in these days of budget cuts and fiscal crises at many municipalities and states, there is little ability of these institutions to pay. In effect, the spectrum to be leased by the managed access system should be considered the wireless carrier's contribution to or investment in solving the problem of contraband device use and as a result, should not be charging for its use.[27] The alternative to leasing the spectrum to managed access

[26] In addition, inmates are federally prohibited from using wireless devices in correctional facilities so CMRS carriers should not be entitled to this revenue regardless. 18 USC § 1791(d)(1)(F) (prohibiting inmates from having, or visitors from providing inmates with, "a phone or other device used by a user of commercial mobile service . . .").

[27] Wireless companies have proved in the past to be civic minded and willing to incur expense for the public good. For example, several major carriers rolled out their Wireless Emergency Alert (WEA) services prior to the implementation deadline and announced various commitments to provide reliable public service in times of public safety crises. *See* Mike Snider, *Cellphones Get Emergency Alerts*, USA TODAY (May 13, 2011) http://usatoday30.usatoday.com/tech/news/2011-05-09-emergency-alerts_n.htm (stating that "AT&T, Sprint, T-Mobile and Verizon – have collaborated to voluntarily initiate the service prior to an April 2012 deadline."). And, the voluntary industry initiatives mentioned above reflect responsible carrier contributions and investments.

providers is for each carrier to build out the solution themselves – which would clearly come at a much higher price.

(4) Model Agreement

Tecore has been through the leasing process for managed access systems multiple times. While, in Tecore's experience, each of the carriers in the areas of the installed systems has been cooperative through the process, having a model spectrum lease available for managed access systems will speed the process of spectrum agreement and approval. A common spectrum sublease, approved by the FCC, that sets forth model terms and conditions for the installation and operation of the managed access system, and the relationship between the carrier and the managed access system operator, would be most helpful.[28] Indeed, there have been prior instances where the FCC has endorsed model agreements that were hammered out by industry groups, and it found them to be "an acceptable accommodation to outstanding issues."[29] This model sublease will provide a template that makes it easier for carriers to promptly accept the lease terms, and will eliminate lengthy negotiation processes. Moreover, the common spectrum

[28] The model sublease should specify certain provisions to define the survivability of the managed access sublease in the event of the expiration of carrier licenses, a carrier's notice of technology change, or network modifications that will impact the managed access operations. The model sublease also should provide a clear definition of sublease termination clause conditions including removal and termination for convenience.

[29] *See In the Matter of Interconnection between Wireline Telephone Carriers and Radio Common Carriers Engaged in the Provision of Domestic Public Land Mobile Radio Service Under Part 22 of the Commission's Rules*, 80 FCC 2d 352, 353 ¶ 5 (1980); *see also In the Matter of Interconnection between Wireline Telephone Carriers and radio Common Carriers Engaged in the Provision of Domestic Public Land Mobile Radio Service under Part 21 of the Commission's Rules*, 63 FCC 2d 87 (1977). Specifically, wireline and paging companies conducted a series of informal meetings to discuss a number of issues associated with interconnection agreements. At the end of the meetings, the parties requested that the Commission approve a Memorandum of Understanding, which the Commission found to be "an acceptable accommodation among all signatories of long-outstanding issues" and something that "should serve as an approach to arrangements between other WTCs and RCCs." 63 FCC 2d at 89, ¶ 12.

sublease will relieve the Commission's concerns regarding the impact this system will have on small and rural operators by assisting these carriers, which may not have the resources to define and execute a unique spectrum lease, and may not otherwise participate in the process.[30]

c. Tecore Agrees With The Commission's Proposed Modifications To Facilitate Lease Agreements Between Wireless Providers And Managed Access System Providers

Tecore applauds the Commission for seeking comment on proposals to streamline the leasing process because speeding up the CMRS licensing process is critical to the acceleration of a managed access system deployment.[31] As earlier noted, one of the most important factors in the implementation of managed access solutions is creating an environment that fosters the prompt entry of commercially reasonable leases. The benefit of that environment will be lost, in part, if spectrum leases languish pending approval. Thus, Tecore strongly agrees with the Commission that certain existing spectrum leasing rules should be modified in the managed access context, while other existing rules are unnecessary due to the nature of these systems.

Specifically, Tecore agrees that the Commission should revise its rules to immediately process *de facto* lease agreements or spectrum manager lease agreements for spectrum used exclusively in managed access systems in correctional facilities.[32] Tecore also supports the Commission's finding that certain existing lease application review rules concerning competitive concerns are "unnecessary" in the managed access context.[33] Tecore further agrees that, while leasing may span the entire commercial spectrum in a given geographic location (*i.e.,* the correctional facility campus), in Tecore's experience, it is unlikely that two managed access

[30] *See NPRM* ¶ 70.
[31] *See id.* at ¶ 24.
[32] *See id.* at ¶ 3.
[33] *Id.* at ¶ 40.

solutions would be deployed in the same area.[34] Therefore, the standard rules and regulations for spectrum leasing and competition should not apply to the unique context of a managed access system. These procedural revisions, as well as the other streamlining proposals made by the Commission, are welcomed by Tecore and will make a significant difference in the time needed for the deployment of managed access solutions.

In addition, managed access spectrum lease applications should be subject to a completeness requirement set forth in existing spectrum leasing rules.[35] Imposing this standard will ensure that the streamlined application review process may begin successfully. In this regard, the Commission should use the modified definition of a managed access system as proposed above by Tecore, including the six criteria that Tecore proposes adding to the definition, in order to determine whether a proposed "managed access system" meets the completeness standard. [36]

Lastly, Tecore supports the Commission's proposal that managed access systems in correctional facilities that are provided on spectrum leased from CMRS providers should be presumptively treated as Private Mobile Radio Services ("PMRS").[37] Tecore agrees that this classification will provide the necessary framework for operating managed access systems because these services are not intended to be services for the public, but instead are for confined specific areas, correctional facilities, and should be recognized as such. Tecore suggests that, as the deployment of managed access evolves, the managed access system operator should be

---

[34] *See id.* (proposing that reviewing existing lease applications for competitive concerns is "unnecessary because managed access systems intended solely to combat contraband wireless devices in correctional facilities do not raise the same competitive concerns as multiple licenses leased in the same geography to provide a CMRS.").

[35] *Id.* at ¶ 39.

[36] The criteria are discussed *supra* Section IV(a).

[37] *NPRM* ¶ 45.

permitted the flexibility to leverage the spectrum in coordination with the CMRS holder to provide local services (that are not available to the public). Tecore feels this allowance is acceptable given that the deployment of managed access is targeted at non-public areas with restricted access. Finally, permitting managed access services to be classified as PMRS without a separate application or approval process will further increase managed access deployment by expediting the administrative requirements involved with these services.

IV. PROPERLY CONFIGURED MANAGED ACCESS SYSTEMS SHOULD BE THE PREFERRED SOLUTION TO COMBAT CONTRABAND WIRELESS DEVICE USE IN CORRECTIONAL FACILITIES

Several solutions currently attempt to address the problem of contraband wireless devices in correctional facilities. However, while other solutions deal in detection, search, and seizure, managed access solutions stand alone as the only legal method of controlling commercial wireless devices within a targeted footprint. In addition, as previously noted, wireless carriers have publicly stated their praise of managed access system solutions. Thus, the Commission should recognize that a fully deployed and properly configured managed access system is clearly the preferred solution to combat the issue of contraband wireless devices in correctional facilities. Tecore recommends that the Commission identify managed access solutions as the preferred approach for eliminating the use of contraband devices in correctional facilities and implement certain technical guidelines that will ensure that managed access systems are properly designed. Moreover, any system analyzing the criteria to classify a device as contraband must be subject to the same exacting standards of coverage footprint as a managed access solution.

a. Managed Access Systems Are Adaptable And Flexible

In order to effectively combat the use of contraband devices in prison, a solution must have the ability to thwart the use of the range of devices and the spectrum bands/frequencies in which these phones operate. Managed access systems are capable of doing so and thus, are ideal

solutions for combating the use of contraband wireless devices in correctional facilities. As the Commission notes, this effectiveness is due, in part, to their ability to "cover the borders of the target area, as well as the technologies and frequency bands of the wireless provider networks . . . through the use of power control, directional antennas, and repeaters."[38] Managed access solutions generally focus on the core group of wireless technologies that are widely commercially available and, within these technologies, all protocols and frequency bands are addressed. As new technology is developed and implemented, managed access solutions are also able to evolve and develop, allowing these solutions to continue to address the evolving contraband device problem at hand.

Managed access systems can also be configured to be free from interference concerns if they are designed properly (as would be required by the FCC under Tecore's proposal).[39] Tecore strongly disagrees with CellAntenna's argument that "detection systems are superior to managed access and jamming systems because detection systems do not threaten to cause interference with carrier networks."[40] Indeed, as the Commission points out, wireless providers "have indicated a preference for managed access solutions . . . on the grounds that [they] 'can effectively prevent unauthorized communications without disrupting legitimate users.'"[41] Thus, it has been demonstrated that managed access solutions are the best alternative for combating the use of contraband wireless devices in correctional facilities.

---

[38] U.S. DEPARTMENT OF COMMERCE, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, CONTRABAND CELL PHONES IN PRISONS: POSSIBLE WIRELESS TECHNOLOGY SOLUTIONS, 19 (Dec. 2010) ("*NTIA Report*").

[39] *Id.* at 2 ("Managed access systems have the potential to cause interference outside of the prison or to adjacent bands *unless properly designed*.") (*emphasis added)*.

[40] *NPRM* ¶ 54.

[41] *Id.* at ¶ 20.

b. Managed Access Systems Can Facilitate Public Safety Services

As recognized in the *NPRM*, it is technically feasible for a managed access system to pass 911 and E911 phone calls through directly to the appropriate PSAP.[42] Managed access systems provide the method for making the decision to allow a call at the subscriber level rather than at the RF signal level, and therefore the system can distinguish the allowed users from those not permitted service. Such an approach will enable the completion of 911 calls while otherwise restricting service, which is a key distinguishing factor from other potential solutions.

Managed access systems can also provide more control over E911 calls and prevent attempts to disrupt the system. For example, managed access systems provide a throttling effect for inbound requests to the PSAP. The capacity for calls from the correctional institution can be limited to the dedicated set of trunks from the facility to the PSAP. Moreover, managed access systems can also provide important public safety data. If the call is presented to the PSAP from the correctional institution location, it will already provide a relative proximity that allows for the location of the site of the call. In many cases, providing the location of the facility is more precise than the location provided in the commercial network. In addition, managed access systems, such as the iNAC, can also provide the type and detail of information that commercial network operators provide. This information may include device identity, the activity record, such as numbers dialed and text messages sent, along with the information necessary for CALEA-compliant interfacing to Law Enforcement Agencies.[43]

---

[42] *Id.* at ¶ 46.

[43] The facilitation of these public safety services rely upon the direct connection between the managed access service and the PSAP. As a consequence, the Commission should not entertain proposed solutions that redirect 911 calls to the commercial carrier for handling. Although this type of system may be technically possible, there are potential security risks associated with such a procedure. For instance, if the calls are redirected, inmates, upon learning of this system, will (continued...)

c. Device Detection And Deactivation Should Only Be Used In Conjunction With Managed Access Solutions – And Only After Further Criteria Are Established By The FCC

Tecore does not support the use of a detection and deactivation system as the only method used by correctional facilities to combat the use of illegal wireless devices. While Tecore agrees that the inclusion of device identification and subsequent deactivation (termination) in the commercial network can be a component of a comprehensive solution, Tecore does not feel that gathering device information via a detection solution, in and of itself, produces an adequate method for deterring the use of contraband cell phones.

As an initial matter, while the detection and location of the device are valuable pieces of information, the amount of time, effort and man power required to physically go to the location and retrieve the device outweighs the benefit of having the information.[44] The accuracy of detection solutions can vary greatly as well. These solutions typically require numerous sensors or receivers to be installed in close proximity to be able to deliver an adequately precise location. Inmates also frequently sabotage and tamper with the necessary sensors and receivers.

Another issue with detection-only systems is that, until the device is confiscated and deactivated, it can still place calls. Deactivation only serves to limit the life of a single contraband device in the correctional facility, and not provide a solution to the overall problem. In fact, the inability of detection solutions to address the growing contraband cell phone issue is

(...continued)

use it as a method to flood the PSAP with 911 calls, disrupting the standard operation of the PSAP and emergency response system. In addition, a redirected device will take additional time to be reacquired on managed access. During this period, it is also possible that an illegal contraband device could place a call on the commercial network before being reacquired. In contrast any solution qualifying as managed access should provide the capability to provide local processing of E911 on the managed access system (not via the commercial signal).

[44] *See NPRM* ¶ 53.

what gave rise to the managed access solutions of today. Therefore, Tecore believes that the inclusion of device identification and deactivation only *as part of* a comprehensive managed access solution is a viable option that the Commission should consider in this proceeding.

In addition to these obvious detection flaws, there are several other challenges that the Commission must consider when evaluating a deactivation system as the solution for contraband device use in correctional facilities. However, as Tecore explains below, many of these challenges can be alleviated by incorporating the detection and deactivation system into the managed access system procedures.

1) Detection And Deactivation Techniques May Pause The Illegal Behavior, But Will Likely Not Eliminate It

The first major challenge for any detection system is that any deactivation solution must target both the SIM card (as applicable), and the device serial number ("IMEI").[45] The commercial network does not typically request the IMEI information, so passive detection systems will not see this information unless the commercial network provokes its transmission. Active detection systems such as IMSI catchers can provoke the transmission of the IMEI information from the device but only by broadcasting in the commercial spectrum to attract the device.

Even if a system is able to gain this information, the information alone cannot block service until the SIM is deactivated. Once the SIM is deactivated, it can be easily replaced for a relatively low cost, and then the whole process must begin again. Furthermore, with respect to

[45] Deactivation of the IMSI only impacts the SIM card, which can be easily replaced. Because most of the contraband devices use prepaid accounts, many times, the refill of the account is accomplished by replacing the SIM card. Unless the solution also includes the capability to deactivate the device (IMEI), the result of the detection is an uptick in the trafficking of replacement SIM cards.

prepaid SIM cards, it is quite possible that the carrier deactivation of the account will happen long after the credited amount on the SIM card is used, rendering the deactivation scenario ineffective. Given the current economics of, and disposable attitude towards SIM cards, it is not clear that the investment in the deactivation process and procedure would make economic sense for the carrier because detection and deactivation, in this sense, are merely pausing the illegal behavior until a new SIM card is purchased or a new device is smuggled into the correctional facility.

However, when a detection and deactivation solution is implemented as a feature of a managed access system, the managed access system controls the device, and, as a result, the device no longer operates on the commercial network. The managed access system can collect device serial number information and SIM card data to provide the IMSI/IMEI[46] (MIN/ESN)[47] combination for the carrier. The IMEI can then be registered in the nationwide Equipment Identity Register ("EIR") effectively disallowing any service in the future to the device. In this case, it will not matter whether or not the SIM card is replaced, because the device will not be functional on the commercial network.

Moreover, a second challenge for detection-only systems is that the contraband devices remain operational while the system determines its contraband status. This delay allows the illegal activity to continue, despite detection of the device. Thus, even if a device is detected and wireless carriers have a hour time limit to terminate the ability of the device to communicate, it is possible that the damage may already have been done. However, if the devices are operating on the iNAC managed access system while the "contraband status" is being determined, there is no

[46] International Mobile Subscriber Identity/ International Mobile Equipment Identifier.
[47] Mobile Identification Number/Electronic Serial Number.

continued activity on the commercial network if the device is controlled by managed access. Indeed, if such detection is part of a managed access system, the managed access provider will have the time to gather the requisite information to determine a device's contraband status, while still maintaining control of the device communications, thereby further eliminating the loopholes the may arise in a detection system.

2) Further Considerations Are Necessary Before Implementing Any Deactivation Solution

To the extent that the FCC adopts any detection and deactivation procedures in conjunction with a managed access solution, there are additional issues that need to be reviewed and considered. Indeed, the Commission must undertake additional inquiries before it implements any proposal "to require CMRS licensees to terminate service to contraband devices within correctional facilities pursuant to a qualifying request from an authorized party."[48]

First, there are several liability concerns associated with the deactivation of contraband devices that must be addressed by the Commission. Overall, the path of liability in the process of deactivating subscriber service must be clearly defined to garner participation from the CMRS providers. Until this participation is regulated (with a clear path of liability for both valid and invalid deactivations), it is unlikely that all CMRS operators will participate. For instance in the event that a SIM card is deactivated, there are potential liability issues associated with the wireless carrier for transactions that occur on the contraband device from the time of their notification from the institution to the time of deactivation. In addition, carriers may also face problems when user subscriptions are deactivated in error.

Second, the termination procedure does not contemplate the jurisdictional issues associated with international devices or domestic roaming devices. For instance, if a device is

[48] *NPRM* ¶ 56.

being used within the United States but has its service subscription provided from an international operator, it is not feasible to expect that the international operator will deactivate the account. For example, if a Vodafone device appears on AT&T's network spectrum inside of a correctional facility in the U.S., how would this service get terminated? Termination would require participation in the deactivation process from, not only all of the domestic wireless carriers, but also all international carriers that roam on the U.S. wireless networks. Gaining this global participation is an unlikely scenario.[49]

Domestically, there is the additional question of jurisdiction. If an inmate in Georgia obtains ten contraband SIM cards from a rural Alaskan operator that roam with the local carrier in Georgia, what is the legal jurisdiction that the Georgia Department of Corrections has to enforce to deactivate the account in the Alaskan operator's system? While the question of deactivation for a nationwide operator like AT&T or Verizon may be easier to answer, if this situation occurs between a state or local correctional facility and a small rural carrier on the other side of the country, who governs this transaction and through what jurisdiction does it operate?

Finally, the Commission must articulate specific information that the correctional facility must transmit to the provider to effectuate termination procedures.[50] Tecore recommends that, at a minimum, the following information be considered: (1) Defined uniform criteria of device information (across technologies) that must be collected to identify the subscription/device to be

[49] Even within the domestic United States it is difficult to see a path to 100% operator participation. Existing regulations ranging from Phase 2 E911 to CALEA have demonstrated a slow deployment cycle due to technology modifications, subscriber notification and other carrier compliance issues. Without full carrier participation, any adopted deactivation technique will not be an effective solution in addressing contraband cell phones. Rather it will only serve to drive those seeking contraband devices to the networks that continue to "work" (*i.e.,* those carriers not participating – whether domestic or international).

[50] *NPRM* ¶ 59.

terminated; (2) defined criteria for reaching the conclusion that a device is contraband; (3) defined interface for transmission of the service subscription to the CMRS from the PMRS site; (4) defined procedure for accepting or rejecting a request; (5) defined timeframe for applying the termination; and (6) defined procedure for protesting and reinstating invalid terminations.

V. TECORE RECOMMENDS PROPER NOTIFICATIONS TO SURROUNDING AREAS OF MANAGED ACCESS SYSTEMS

Tecore agrees with the FCC that a key component of a managed access solution should be the notification of the households and businesses in the general vicinity of a correctional facility where such a solution is in place. Managed access systems are installed as a measure of national security and the surrounding public should be made aware of the system. Notification can also serve to limit the liability of the carriers, the institutions, and the managed access operator with the general public.[51]

With respect to the form of notification, Tecore cautions the Commission against implementing any requirements that may be burdensome or counterproductive. Tecore supports a standard method that will be easily achieved by the managed access service provider. For instance, a standard method of posting a public notice in a common area, posting notification to a country, state or other local website, or even a displaying signs on the grounds would be sufficient. Tecore also recommends that the Commission adopt a requirement that such notice must protect managed access system providers, as well as wireless provider lessors, from any

[51] As noted above, these systems are put in place for the greater good of the public and should not be subject to frivolous lawsuits and legal action as long as the efforts of the institution, the operator, and the commercial carriers are reasonable to contain the service within the walls of the institution.

liability that may potentially result from the unlikely event that a non-contraband wireless device is picked up and blocked in the vicinity of the managed access system.

VI. CONCLUSION

For the above stated reasons, Tecore respectfully requests that the Commission adopt managed access systems as the preferred solution for combating contraband wireless devices in prisons.

Respectfully submitted,

Tecore Networks

/s/ Carl W. Northrop

By:

Carl W. Northrop
Michael Lazarus
Jessica DeSimone
Telecommunications Law Professionals PLLC
875 15th Street, NW
Suite 750
Washington, DC 20005
Telephone: (202) 789-3120
Facsimile: (202) 789-3112

Its Attorneys

Jay Salkini
Chief Executive Officer

Casey Joseph
Chief Technology Officer

Tecore Networks
7030 Hi Tech Drive
Hanover, MD 21076
Telephone: (410) 872-6238
Facsimile: (410) 872-6010

July 18, 2013